UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/736,717	12/12/2000	David Michael Kurn	20206-036 (P00-3418)	8320

7590 10/01/2004	EXAMINER
Hewlett-Packard Company Intellectual Property Administration P.O. Box 272400 Fort Collins, CO 80527-2400	JACKSON, JENISE E

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9 and 10* is/are rejected.

7)☒ Claim(s) *8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *6*

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

2.   Claims 1-7, 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van

Oorschot(6,317,829) in view of Eastlake.

3.   As per claim 1, Van Oorschot discloses a cryptographic keys used during operation of a

computer system(see col. 3, lines 20-24), providing an old set of cryptographic keys(see col. 6,

lines 21-32, col. 7, lines 3-14); checking with a key repository to determine if a certificate re-

issuance is necessary, meanwhile maintaining the availability of the old set of cryptographic

keys(see col. 6, lines 22-32, col. 7, lines 3-14); the new keys are stored in the database(see col. 4,

lines 24-48, col. 7, lines 6-11), providing the new or revised keys to applications that need them

when next requested by such applications(see col. 3, lines 30-39, col. 6, lines 22-32). Van

Oorschot discloses an application, because the primary computing unit, and the server

communicated the key history information via a internet link(see col. 5, lines 3-6), an application

is inherent in Van Oorschot, because Van Oorschot discloses communicating the key

information to the primary computing device via an Internet link, this link has an application,

such as a web browser. However, Van Oorschot does not disclose key rollover. Eastlake does

disclose key rollover.

4.   It would have been obvious to one of ordinary skill in the art at the time of the invention

to combine Van Oorschot with Eastlake to include key rollover, one would have been motivated

to include key rollover of Eastlake, because in order to obtain high levels of security, keys must

be periodically changed, or "rolled over"(see pg. 3 of Eastlake). Rollover is necessary because

the longer a private key is used the more likely it is to be compromised due to cryptanalysis,

accident or treachery(see pg. 3 of Eastlake).

5.   As per claim 2, Van Oorschot discloses key repository utilizes one or more services of a

specialized application acting as an extension of the key repository (col. 3, lines 27-39, col. 6,

lines 22-32).

6.   As per claim 3, Van Oorschot discloses the key repository utilizes the one or more

services of the specialized application, authenticating authorization of the specialized application

to perform those services(see col. 3, lines 27-39, 51-67, col. 7, lines 30-53).

7.   As per claim 4, Van Oorschot discloses a command that when the key is about to

approach expiration, a new key is issued(see col. 6, lines 22-32). Van Oorschot does not disclose

invoking the command. Eastlake discloses invoking a key rollover. The motivation to include

invoking the key rollover, is that being invoked as a result of a command, is the longer a private

key is used, the more likely it is to be compromised due to cryptanalysis, accident or

treachery(see pg. 3 of Eastlake).

8.   As per claim 5, Van Oorschot discloses a periodic check which senses that the old set of

cryptographic keys are approaching expiration (see col. 4, lines 24-47, col. 6, lines 21-32).

9.   As per claim 6, Van Oorschot discloses a result of sensing an expired key(see col. 4, lines

24-47, col. 6, lines 21-32).

10.   As per claim 7, Van Oorschot discloses wherein the applications are notified of the presence of new keys by the key repository process(see col. 8, lines 41-56).

11.   As per claim 9, Van Oorschot discloses wherein the key repository process is prompted by the applications to invoke the method as a result of the applications detecting a key approaching expiration (see col. 6, lines 62-67, col. 7, lines 1-11).

12.   As per claim 10, Van Oorschot discloses wherein the applications request the key repository process to provide a new key as a result of applications detecting an expired key(see col. 7, lines 1-14).

13.   Claim 8 it is objected to as being rejected on base claim, Claim 8 is allowable for the feature of an application detecting a missing key, and check with the key repository for that key and, if the missing key has been reissued, the applications receive a newly-issued key, the prior art of digital certificates and revocations, discloses that if a key is missing or lost, that the key can be recovered through various cryptographic techniques. In prior art it does not disclose that if a key is missing, reissuing another key.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100